REMARKS/ARGUMENTS

In view of both the amendments presented above and the following discussion, the Applicants submit that none of the claims now pending in the application are anticipated under the provisions of 35 USC § 102 (e) or obvious under the provisions of 35 USC § 103 (a). Thus, the Applicants believe that all of these claims are now in allowable form.

Reexamination and reconsideration of the application as amended are respectfully requested. If, however, the Examiner believes that there are any unresolved issues in any of the claims now pending in the application, the Examiner should telephone Ms. Janet M. Skafar, Esq. at message telephone number (408) 463-5670 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Status of Claims

Claims 1, 4, 6, 7-12, 15-20, 23, 26, 28, 29-34, 37-42 have been amended. Claims 13, 14, 21, 22, 35, 36, 43 and 44 have been canceled. No new claims have been added. Claims 1-12, 15-20, 23-34, 37-42 remain pending in this application.

Claim Rejections under 35 U.S.C. § 102 (e)

Claims 1-4, 7-10, 15-18, 23-26, 29-32 and 37-40 have been rejected as being anticipated by Mitty et al. US Patent No. 6,145,079 ("Mitty"). Applicants respectfully disagree and traverse the rejection.

Applicants have amended independent claims 1, 7, 15, 23, 29 and 37. The rejection will be discussed with reference to method Claim 7. Applicants submit that Mitty does not teach all the limitations of claims 1, 7, 15, 23, 29 and 37. In particular, Applicants maintain that Mitty does not

teach "recovering said decrypting of said encrypted data element without retransmission of data." Therefore, Applicants submit that the Mitty patent does not anticipate Claim 7.

Independent claims 1, 15, 23, 29 and 37 contain limitations similar to Claim 7, and are not anticipated for the same reasons as Claim 7. Claims 2-4, 8-10, 16-18, 24-26, 30-32 and 38-40 depend from Claims 1, 7, 15, 23, 29 and 37, respectively, and are not anticipated for the same reasons as Claim 7.

Furthermore, independent Claim 29 has additional limitations not taught by Mitty. Claim 29 recites "encrypting said static encrypted data element chunks with said dynamic key to provide dynamic-static data element chunks and dynamic encryption recovery information states", and recovering, on said receiving computer system, said decrypting of said dynamic-static data element chunks after said one of said dynamic-static data element chunks based on one of said dynamic encryption recovery information states." Mitty does not teach "dynamic encryption recovery information states" and does not teach recovering said decrypting of said dynamic-static data element chunks based on one of said dynamic encryption recovery information states."

Claim Rejections under 35 U.S.C. § 103(a)

Claims 12-13, 20-21, 34-35 and 42-43 have been rejected as being unpatentable over Mitty in view of Koopman Jr. et al (Koopman). RE36,181. The rejection asserts that "Mitty teaches the determination of whether a transmission failed (Mitty Col. 6, lines 30-56, confirmation messages) but fails to teach the repairing of the data element without retransmission." [Office Action, Page 7]. The rejection asserts that Koopman teaches the repairing of the data element without retransmission (Koopman, col. 16, lines 44-56). "Koopman teaches pseudorandom number generation system with cryptographic authentication." [Office Action, Page 7]. Applicants respectfully disagree and traverse the rejection.

Claims 13, 14, 21, 35 and 43 have been canceled and independent Claims 1, 7, 15, 23, 29 and 37 have been amended to include the limitation of recovering said decrypting.

Applicants submit that the combination of Mitty and Koopman, explicitly or implicitly, does not teach the claimed invention of Claims 1, 7, 15, 23, 29 and 37. In the response to arguments, the Examiner indicated that the type of environment is not positively recited in the claims. Applicants respectfully point out that a streamed environment is recited in claims 23, 29, and 37 which recite that a data element is partitioned into a plurality of chunks, and recite data element chunks.

Mitty teaches an electronic messaging system, requiring a non-streamed (non-chunked) environment with the entire data contents, envelope and contents, available. [Mitty, Abstract] "There is a need in the art for an electronic message system that provides privacy, authentication of participants, and non-repudiation." [Mitty, Col. 2, lines 1-3] Mitty teaches secure electronic transmissions that are applied to "packages" that include the entire data contents.

> "Using techniques described below, sender 105 transmits a "package" to a trusted intermediary 115 via potentially non-secure network 110, such as the Internet." [Mitty, Col. 6, lines 26-27] "In short, both the original and new version of the package have an inner and outer "digital envelope." These digital envelopes are instances of envelopedData, and information they contain enable the system to provide privacy, authentication, and non-repudiation." [Mitty, Col 6, lines 57-61]

In contrast, Applicants' invention, in claims 1, 7, and 15, operates in either a chunked or non-chunked environment thereby improving performance of the transmission of encrypted data. Furthermore, Applicants' invention in claims 23, 29 and 37 is expressly directed towards a chunked environment. It would not have been obvious to one skilled in the art to attempt to extend the teachings of Mitty from an electronic messaging system supporting non-chunked data, to a system supporting video stream data or chunk data. Applicants' invention enhances performance of encryption and decryption of data elements by operating on chunked or non-chunked data. For example,

> The data 103 used and created on the data server 102 may be stored in computer-readable media data storage 116. The dynamically encrypted data 114 is typically not stored on permanent storage, such as computer disks. For example, the dynamically encrypted data 114 may be stored in computer memory. Further, the dynamically encrypted data 114 may be partitioned into chunks and each chunk may be processed

> with the use of computer memory thereby climinating storage during the operation of the present invention. (Specification, page 11, lines 5-11)

Further, it would not have been obvious to one skilled in the art to extend the teachings of Mitty that require the entire data contents to be used in the encryption and decryption process, to a chunked environment that does not require availability of all the contents contained within an envelope. More particularly, the focus of Mitty is an electronic messaging system, which is not similar to the focus of Applicant's invention of claims 1, 7, and 15, that operates in either a chunked or a non-chunked, streamed data, environment. For example, Applicants' invention enables such a flexible, high-performance solution that operates with some personalized or dynamic features typically associated with chunked dynamically encrypted data.

Koopman is directed to a different problem from the claimed invention. Koopman focuses on automobile door lock receiver ("keychain fob") encryption technology, while Applicants' invention is directed to state recoverability of encryption systems. For example, Applicants' invention teaches recovery of an unreliable channel as follows,

> Third, if an unreliable channel is used, the data decryption method 504 requires a way to recover the state, "s," 604 in order to decrypt the data 103 that follows the transmission loss. That is, the data decryption method 504 includes state recoverability information in the form of the state, "s," 604. The method of saving the state, "s," 604 is described with reference to elements 525 and 527 in Figure 5B. The method of extracting the state, "s," 604 is described with reference to element 568 in Figure 5C.
>
> Fourth, if the static encryption requires maintenance of the state, "s," 604 to enable decryption, either the transmission channel between the encrypting computer system and the decrypting computer system should be reliable or the method of data decryption 504 should enable recovery of the state, "s," 604. To enable recoverability, the payload buffer size, "p," 606 is typically the size of the data 103 presented in a buffer plus the size of the state, "s," 604 for encryption with a static key 108. [Specification, page 19, lines 6 – 19]

Combining the teachings of Mitty with the error correction code detection of Koopman [Col. 16, lines 43-56] would not result in the Applicants' claimed invention of recovering decrypting of said data element without retransmission of data of Claims 1, 7, 15, 23, 29 and 37. Koopman relies on error correction that is a "single error" correction, ". . . correcting any single error which can be

fixed". [Koopman, Col 16, lines 47-48]. The claimed invention is not single bit error correction. The claimed invention recovers decrypting of the data element without retransmission of data. Therefore, the combination of Mitty and Koopman would not result in the claimed invention.

Furthermore, Claim 29 recites further distinguishing limitations. The dynamic encryption recovery information state of Claim 29 of Applicants invention is completely different from the error correction code and single bit error correction of Koopman. In Applicants claimed invention of Claim 29, the dynamic encryption recovery information state is transmitted with the static-dynamic encrypted data and is used to recover the state of the encrypted data in order to properly decode subsequent data. A payload buffer that is lost is not corrected using an error correction code; however the encryption recovery state allows decryption of subsequent payload buffer data to continue to be performed properly. "The present invention saves the state, "s," 604, in the encryption processing loop 520, thereby enabling recoverability of a lost payload buffer, "B," 602. Recoverability via use of a state enables decryption to continue without re-transmitting a buffer if it is lost. Therefore, the present invention transmits the saved state, "s," 604 to the client computer system 150 (as shown in FIG. 1). The purpose of including the saved state, "s," 604 in the same transmission as the encrypted payload buffer, "B," 602 is to ensure that decryption is successful even if an individual payload buffer, "B," 602 is lost. Those skilled in the art will appreciate that the saved state, "s," 604 is a value that represents the state at the time immediately preceding the encryption of the payload buffer "B," 602. It will be appreciated that the process of encrypting a buffer changes the state. When any data element 103 within the payload buffer "B," 602 is corrupt the entire payload buffer "B," 602 is considered corrupt. The output of encryption is the input for the decryption operation. If the output channel, "N," 610 is unreliable, as shown in element 524, the state, "s," 602 is prepended to the payload buffer "B," 602 as shown in element 525. The initial state, "s," 604 is saved during the operation of the initialization method 515 (as shown in FIG. 5A). As shown in element 526, the current state of the encrypted payload buffer, "B," 602 is saved into the state, "s," 604." (Applicants' Application, paragraph 77). The present invention uses the saved state "s," 604 to recover the state of the encrypted information. (Applicants' Application, paragraph 83). Therefore, if a data element chunk is lost or corrupted, without the saved state, the data element chunk, and subsequent data elements chunks would not be decrypted properly. Using the saved state in the payload of a subsequent data element chunk, that data element chunk and following data

element chunks can be decrypted. Therefore, decrypting of data elements chunks can continue, in other words, decrypting is recovered.

For the foregoing reasons, Applicants submit that Claim 29 is non-obvious. Therefore Applicants respectfully request that that Claims 1, 7, 15, 23, 29 and 37, be allowed. In addition, Claims 12, 20, 34 and 42 depend from Claims 1, 7, 15, 23, 29 and 37, and are non-obvious for the same reasons as Claims 1, 7, 15, 23, 29 and 37, respectively.

Claims 5 and 27

Examiner has rejected Claims 5 and 27 as being unpatentable over Mitty et al. "With regards to Claim 5 and 27, Mitty fails to teach the second computer being untrusted." Examiner contends that untrusted computers are well known in the art and it would have been obvious to a person of ordinary skill in the art to allow Mitty's system to work with untrusted computers because it offers the advantage of allowing interoperability with a far wider range of networks and systems. [Office Action, page 6]

However, Applicants have amended the independent claims. Because, as discussed above, Mitty does not all the limitations of claimed invention, the Applicants submit that a prima facie case of obviousness has not been met.

Furthermore, Examiner has indicated that the motivation for allowing Mitty's system to work with untrusted computers is because it offers an advantage of allowing interoperability with a far wider range of networks and systems. Mitty requires the use of a trusted intermediary. [Mitty, Col 2, line 12] Applicant's invention does not require a trusted intermediary, working on streamed, or chunked data, with either a trusted or an untrusted computer system. It would not have been obvious to one skilled in the art to use an untrusted computer as is taught by Applicants' invention, because the techniques of Applicants' invention were not known at the time the invention was conceived. Part of the problem in the past was that such features required and relied upon a trusted computer

intermediary. Therefore, an aspect of the novelty of Applicants' invention is that it operates on chunked or non-chunked data and does not require a trusted computer system.

Fore the foregoing reasons, Claims 5 and 27 are not obvious; and reconsideration and allowance of Claims 5 and 27 is respectfully requested.

Claims 6, 11, 19, 28, 33 and 41

Claims 6, 11, 19, 28, 33 and 41 are rejected as being unpatentable over Mitty in view of Bailey III US Patent No. 5,659,614 ("Bailey"). The rejection asserts that Mitty teaches the limitations of Claims 6, 11, 19, 28, 33 and 41 with the exception that Mitty, "fails to teach the data element being decrypted by the same dynamic key on a second computer system." [Office Action, Page 7] "Bailey teaches the data element being decrypted with the static key and the dynamic key on a second computer system [Bailey, column 6 lines 9-21, column 18 lines 53-55] [Office Action, Page 7]

Claims 6, 11, 19, 28, 33 and 41 are dependent on independent Claims 1, 7, 15, 23, 29 and 37, respectively. For all the reasons put forth with respect to independent Claims 1, 7, 15, 23, 29 and 37, Applicants submit that Claims 6, 11, 19, 28, 33 and 41 are not obvious over Mitty. Further, Bailey is focused on decryption at a backup site and is related to file data, not chunked data, as expressly recited in Claims 23, 29 and 37. Bailey is directed to "A method and system for prioritizing, securing, and reducing the amount of data transmitted and stored during the creation of a backup copy of file data." [Bailey, Abstract]. In contrast, the claimed invention is directed to the accelerated dynamic protection of data. Further, Bailey requires a data security card for additional numbers to serve as keys (Col. 18, lines 30-44) and this technique is not similar the techniques of Applicants' invention. Therefore, one skilled in the art would not look to the Bailey patent to solve the problem of accelerating the dynamic protection of data. Hence, it would not have been obvious to one skilled in the art to use the techniques of Bailey that are focused on backup techniques for file data, for the purpose of rendering obvious Applicants' invention. For the foregoing reasons, Applicants respectfully request that that Claims 6, 11, 19, 28, 33 and 41 be allowed.

Conclusion

For the foregoing reasons, Applicants submit that the pending Claims 1-12, 15-20, 23-34, 37-42 are patentable over the art of record.

Applicants therefore respectfully request that the Examiner reconsider all currently outstanding rejections and that they be withdrawn. It is believed that a full and complete response has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this Application, the Examiner is invited to telephone the undersigned at the number provided. Prompt and favorable consideration of this Response is hereby solicited.

Respectfully submitted,

August 29, 2005

Janet M. Skafar, Attorney
Reg. No. 41,315
Correspondence Customer No. 24852
Message Telephone: (408)463-5670
Facsimile: (408) 463-4827